TENNESSEE DEPARTMENT OF HEALTH
POLICY ACKNOWLEDGEMENT

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) and CONFIDENTIALITY POLICY

By signing below, I am acknowledging my awareness of the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and acknowledge and understand that, as a member of the Tennessee Department of Health's workforce I am prohibited from releasing to any unauthorized person any protected health information which may come to my attention in the course of my duties. Moreover, I acknowledge and understand that any breach of confidentiality, patient or otherwise, resulting from my written or verbal release of information or records is strictly prohibited except in the course of business.

DRUG-FREE WORKPLACE POLICY

I, as a State employee of the Tennessee Department of Health, or as a County, Contract, or Municipal employee working for the Tennessee Department of Health, or as a volunteer, hereby certify that I have received a copy of the Tennessee Department of Health's policy regarding the maintenance of a drug-free workplace, and by signing below, I acknowledge that I have agreed to comply with the Drug-Free Workplace Policy of the Tennessee Department of Health.

CONFLICT OF INTEREST POLICY

By signing below, I acknowledge that I have read and agree to comply with the Conflict of Interest Policy of the State of Tennessee and the Tennessee Department of Health.

OPERATION OF MOTOR VEHICLES BY STATE EMPLOYEES POLICY

By signing below, I acknowledge that I have read and agree to comply with the Operation of Motor Vehicles Policy.

ACCEPTABLE USE POLICY

By signing below, I acknowledge that I have read and agree to comply with the Acceptable Use Policy Network Access Rights and Obligations Policy.

_____	_____	_____
Signature	Last Four (4) Digits of SS#	Date
_____	_____	_____
Print Name	Supervisor's Signature	Date

*State _____ Driver's License Number _____ Expiration Date _____
(*Required for employees in positions requiring a valid driver's license.)

Failure to comply with the policies listed above may lead to disciplinary action, up to and including dismissal from state service.

Tennessee Department of Health

HIPAA Policies

Privacy

Policy Title: Administrative Requirements for the Implementation of HIPAA

Policy Number: 101

Effective Date: April 14, 2003

PURPOSE:

To issue instructions to all bureaus, offices, programs and workforce members regarding the Department of Health's (DOH) obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §§1320d-1329d-8, and regulations promulgated thereunder, 45 CFR Parts 160 and 164. This policy outlines DOH general guidelines and expectations for the necessary collection, use, and disclosure of protected health information (PHI) about clients in order to provide services and benefits to individuals while maintaining reasonable safeguards to protect the privacy of their information.

Definitions:

Protected Health Information (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Workforce Members means employees, volunteers, trainees, contractors, and other persons whose conduct, in the performance of work for the department, its offices, or programs is under the direct control of the department, office, or program regardless of whether they are paid by the DOH.

Client for the purpose of HIPAA is defined as an individual for whom the DOH uses or maintains protected health information such as:

1. birth and death records,
2. infectious disease records,
3. health registries,
4. statistical data,
5. information obtained through an investigative or certification process of the DOH, etc., and
6. those who apply for or receive health services through DOH.

Licensee is a person or entity that applies for or receives 1) a license, 2) a certification, or 3) a registration, or similar authority from DOH to perform or conduct a service, activity or function.

Provider is a person or entity who may seek reimbursement or payments from DOH as a provider of services to DOH clients. (Not pertaining to DOH when DOH is a direct provider of services)

Treatment, Payment and Health Care Operations (TPO) includes all of the following:

- *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
- *Health Care Operations* include functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services, and auditing functions, business planning and development, and general business and administrative activities.

POLICY:

General Overview

DOH may collect, maintain, use, transmit, share and/or disclose information about clients, providers, and licensees, to the extent needed to administer DOH programs, services and activities. DOH will safeguard all PHI about clients, providers, and licensees, inform clients, providers, and licensees about DOH'S privacy practices and respect clients', providers', and licensees' privacy rights, to the full extent required under this policy.

This policy identifies two types of individuals of whom DOH is most likely to obtain, collect or maintain individual information:

i) DOH clients;

ii) Licensees or providers.

DOH, its workforce, and business associates will respect and protect the privacy of records and information about clients who request or receive services from DOH and licensees and providers. All information must be safeguarded in accordance with DOH privacy policies and procedures.

DOH has adopted reasonable policies and procedures for administration of its programs, services and activities. If any state or federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon any DOH policy regarding the privacy or safeguarding of information, DOH shall act in accordance with the stricter standard.

DOH staff shall act in accordance with established DOH policy and procedures regarding the safeguarding of client information, whether health-related or not, in all DOH programs, services and activities. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, the DOH employee will seek guidance from supervisors according to established DOH policy and procedures. DOH staff should consult with their Subsidiary Privacy Officer or the Department Privacy Officer in appropriate circumstances.

DOH Notice of Privacy Practices

A. The current "***DOH Notice of Privacy Practices***" shall be available in all offices of the DOH.

B. DOH will provide a copy of the current "***DOH Notice of Privacy Practices***" to any client who requests a copy. However, where DOH is a direct provider to the client, DOH is required to give a copy of the notice to the client on the first date that they receive services on or after April 14, 2003. DOH must have each client who receives direct care from DOH sign an acknowledgment of receiving the notice on their first date of service. If DOH cannot get a signed acknowledgement, then documentation as to the reason why one was not received must be made in the client's record. Acknowledgment of receipts of the notice, and/or documentation of good faith effort to obtain written acknowledgement must be maintained for six years.

C. The "***DOH Notice of Privacy Practices***" shall contain all information required under federal regulations regarding the notice of privacy practices for protected health information under HIPAA.

D. The "***DOH Notice of Privacy Practices***" shall also be available at the DOH website.

E. Whenever the notice is revised, it should be made available upon request and posted on or after the effective date of revision.

F. Copies of the notice and all revisions shall be maintained by the Department Privacy Officer.

Administrative Requirements

Due to HIPAA requirements, DOH has implemented certain administrative requirements as specified below:

A. Personnel Designations

1. Department Privacy Officer: The DOH must designate an individual to be the Department Privacy Officer, responsible for the development

and implementation of department-wide policies and procedures relating to the safeguarding of PHI.

2. Subsidiary Privacy Officers will be appointed to represent bureaus/ offices, regional office and local health departments, and to act in support of the Department Privacy Officer.

B. Privacy Officers Duties

1. The Department Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of, and adherence to the department's policies concerning privacy. Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints. Ensure that the Department is 1) in compliance with its privacy practices, and 2) consistently applies sanctions for failure to comply with privacy policies for all individuals in the Department's workforce and business associates.

2. Subsidiary Privacy Officers will be responsible for providing information about DOH'S privacy practices and receiving complaints relating to PHI and forwarding these to the Department Privacy Officer.

C. Workforce Training Requirements

The DOH and, as applicable, its bureaus/offices must document the following training actions:

1. On or before April 14, 2003, all DOH workforce members must receive HIPAA awareness training. Training regarding appropriate policies and procedures relating to PHI will be given as necessary and appropriate for those employees whose jobs are impacted by HIPAA.

2. After April 14, 2003, each new workforce member, or a workforce member reporting to work for the first time since April 14, 2003, shall receive the training as described above within a reasonable time after joining or re-joining the workforce.

3. After training as described above has been given to all the current workforce, DOH shall require every workforce member to sign a

revised "Confidentiality Statement" (Form PH. 3131). All new workforce members shall sign the "Confidentiality Statement" as soon as they have received the appropriate training as outlined above.

4. Each workforce member must receive training as described above within a reasonable time when:

   a. a material change in the policies and procedures relating to PHI occurs and it impacts his/her work, or

   b. a change in jobs or position responsibilities occurs.

D. Policies and Procedures

NOTE: The HIPAA Privacy Policies become effective on April 14, 2003. However, a reasonable time will be given bureaus/offices to become completely compliant with these policies in their program areas. Each bureau/office shall strive to achieve compliance in all areas as soon as feasible.

The DOH and, as applicable, its bureaus/offices must document the following actions relating to its policies and procedures:

1. The DOH shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations to be followed by all workforce members.

2. The DOH must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. The DOH may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, DOH must make correlative changes in its privacy notice. The DOH may not implement a change in policy or procedure prior to the effective date of the revised privacy notice when required.

3. The DOH, and each bureau/office must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the HIPAA regulations, for a period of six (6) years from the later

of the date of creation or the last effective date or such longer period that may be required under state or other federal law.

4. Policies and procedures have been developed for the following administrative requirements:

   a. Safeguarding PHI from intentional or unintentional unauthorized use or disclosure as outlined in **DOH HIPAA Policy #105,** *"Administrative, Technical, and Physical Safeguards."*

   b. Complaint process for documenting and referring complaints received by clients as outlined in **DOH HIPAA Policy #102,** *"Clients' Privacy Rights."*

   c. Application of sanctions and documentation of the application of appropriate sanctions against workforce members as outlined in **DOH HIPAA Policy #109,** *"Enforcement, Sanctions, and Penalties for Violations of Individual Privacy."*

   d. Each bureau/office must mitigate, to the extent practicable, any inappropriate use or disclosure of PHI by DOH or any of its business associates as outlined in **DOH HIPAA Policy #110,** *"Mitigation Efforts."*

   e. Neither the DOH nor any bureau/office or workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of his/her rights relating to HIPAA compliance nor will DOH require clients to waive their rights to file a complaint as a condition for providing treatment, payment, or receiving a service, as outlined in **DOH HIPAA Policy #102,** *"Clients' Privacy Rights."*

5. Policies and procedures for other aspects of HIPAA have been developed to address operational issues as follows:

   a. Clients' rights to access their own information, with some exceptions, as well as the client's right to request restrictions or amendments to their information is outlined in **DOH HIPAA Policy #102,** *"Clients' Privacy Rights."*

b. The requirements DOH needs to follow regarding the uses and disclosures of client information is outlined in **DOH HIPAA Policy #103,** *"Uses and Disclosures of Client Information."*

c. DOH will use or disclose only the minimum necessary information necessary to provide services and benefits to clients as outlined in **DOH HIPAA Policy #104,** *"Minimum Necessary Information."*

d. DOH may use or disclose client's information for research purposes as outlined in **DOH HIPAA Policy #106,** *"Use and Disclosure for Research Purposes and Waivers."*

e. DOH staff will follow standards under which client information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set as outlined in **DOH HIPAA Policy #107**, *"De-identification of client information and Use of Limited Data Sets."*

f. DOH may disclose protected health information to business associates with whom there is a written contract or memorandum of understanding as outlined in **DOH HIPAA Policy #108,** *"DOH Business Associates."*

STATE OF TENNESSEE
DEPARTMENT OF HEALTH
CORDELL HULL BLDG.
425 5TH AVENUE NORTH
NASHVILLE TENNESSEE 37247

PHIL BREDESEN
GOVERNOR

KENNETH S. ROBINSON, M.D.
COMMISSIONER

DATE: December 16, 2004

TO: Bureaus, Regions and Divisions

FROM: Kenneth S. Robinson, M.D., Commissioner

SUBJECT: Drug-Free Workplace Act of 1988

On November 18, 1988, President Ronald Reagan signed the Anti-Drug Abuse Act of 1988. The provisions of this Act will affect all recipients of Federal Assistance.

Specifically, the Act requires all applicants/recipients of Federal Assistance awards made on or after March 18, 1989, to certify as a precondition of any assistance award, that they will provide and maintain a drug-free workplace by taking action to meet certain basic requirements including the following:

1. Completion of a drug-free compliance certificate that certifies that the department is meeting all requirements of the Act;

2. Establishment and publishing of a drug-free workplace policy notifying employees that the unlawful manufacture, distribution, dispensation, possession or use of a controlled substance in the state's workplace is prohibited and specifying the actions that will be taken against individuals found in violation;

3. Specific notification to any employee whose salary is funded, in total or part, with federal funds that they must abide by the terms of the policy statement as a condition of employment or be faced with penalties as set forth in the policy;

4. Establishment of a drug-free awareness program; and,

5. Notification to the federal granting authority of any employee who has been criminally convicted of a drug offense occurring in the workplace.

In order that all departments of state government might be consistent in complying with this Act, the Tennessee Department of Personnel has issued the attached information which sets forth the policy statement and procedures that are to be followed. I have accepted this policy statement and procedures that are to be followed. I have accepted this policy statement as being the policy for this department and it should be properly distributed to each of your employees as well as being posted in a conspicuous place in your facility. There is also an acknowledgement statement to be signed by each employee for compliance to this policy included in the new employee welcome packet.

It is essential that in order that federal funds available to this department not be jeopardized that we comply with this policy. Therefore, I request your usual cooperation.

DRUG-FREE WORKPLACE POLICY

Illegal and excessive use of drugs has become an epidemic in our state. Any abuse and use at the workplace is subject of immediate concern in our society. From a safety perspective, the users of drugs may impair the wellbeing of all employees, the public at large, and result in damage to state property. Drug use may also seriously impair an employee's ability to perform his or her job; therefore, it is the policy of the State of Tennessee that the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance in the state's workplace is prohibited. Any employees violating this policy will be subject to discipline up to and including termination. The specifics of this policy are as follows:

1. The unlawful manufacture, distribution, possession, or use of a controlled substance is prohibited in or on the workplace. Such manufacture, distribution, possession, or use while on the job or state property will subject the violator to discipline up to and including termination.

2. The term "controlled substance" means any drug listed in 21 U.S.C. 812 and other federal regulations. Generally, these are drugs which have a high potential for abuse. Such drugs include, but are not limited to, Heroin, Marijuana, Cocaine, PCP, and "Crack". They also include "legal drugs" which are not prescribed by a licensed physician to an alleged violator.

3. Each employee is required by law to inform this agency within five (5) days after he or she is convicted for violation of any federal or state criminal drug statute where such violation occurred on state property. A conviction means a finding of guilt (including a plea or nolo contendre) or the imposition of a sentence by a judge or jury in any federal or state court.

4. The Tennessee Department of Health must then notify the U.S. government agency with which the grant was made within ten (10) days after receiving notice from the employee or otherwise receiving actual notice of such a conviction.

5. If an employee is convicted of violating any criminal drug statute while on the workplace, he or she will be subject to discipline up to and including termination. Alternatively, the Department may require the employee to successfully finish a drug abuse program sponsored by an approved private or governmental institution.

6. As a condition of employment or continued employment of any federal government grant, the law requires all employees to abide by this policy.

THE POLICY STATED HEREIN IS BEING ADOPTED BY THIS AGENCY IN COMPLIANCE WITH THE DRUG-FREE WORKPLACE ACT.

TENNESSEE DEPARTMENT OF HEALTH
CONFLICT OF INTEREST POLICY

1. ***PURPOSE:*** To assure that an employee's activities do not conflict or have the appearance of conflicting with the provision of full unbiased service to the public.

2. ***APPLICABILITY:*** This policy shall apply to all full-time employees of the Tennessee Department of Health.

3. ***DEFINITIONS:***

   3.1 **CONFLICT OF INTEREST:** a situation in which an employee's activities impair, or give the appearance of impairing, the person's ability to provide full unbiased public service.

   3.2 **SUBSTANTIAL FINANCIAL INTEREST:** ownership by an employee or by the employee's spouse of ten percent (10%) or more of the stock of a corporation or ten percent (10%) or more of any other business entity.

   3.3 **ORGANIATIONAL UNIT:** a subdivision designated by the Commissioner of Health for administrative purposes.

4. ***CONDUCT WHICH CREATES A CONFLICT OR THE APPEARANCE OF A CONFLICT:***

   4.1 An employee shall not engage in any conduct, employment, or other activity which impairs, or gives the appearance of impairing, the person's ability to provide full unbiased public service.

   4.2 An employee shall not violate applicable state or federal laws concerning conflict of interest.

   4.3 An employee shall not knowingly take any action which might prejudice the department's interest in a civil or criminal case.

5. ***FINANCIAL INTERESTS:***

   5.1 It is a conflict of interest for an employee, who has a public duty to recommend, approve, disapprove, monitor, regulate, investigate, or superintend, in any manner, a contract or other activity, to have a substantial financial interest in a business that does, or seeks to do, business with the employee's organizational unit.

   5.2 An employee shall not have a financial interest in an outside entity of such significance that the departmental responsibilities and duties of the employee cannot be rendered in a fair and impartial manner.

   5.3 An employee shall not engage in a financial transaction for personal gain relying upon information obtainable solely through one's employment.

   5.4 An employee shall not receive any compensation from a private source for services which are, or should be, performed as part of one's official duties, except as provided by statute or as approved by the Commissioner.

6. *OUTSIDE EMPLOYMENT AND ACTIVITIES:*

6.1 An employee who has a public duty to recommend, approve, disapprove, monitor, regulate, investigate, or superintend program activities shall not engage in outside employment with an entity that is regulated by the employee's organizational unit.

6.2 An employee shall not serve on a board of directors for a non-state agency that is regulated by, or that has or seeks funding from, the employee's organizational unit unless the Commissioner deems such to be in the Department's interest and grants a waiver of this restriction.

7. ***GIFTS AND FAVORS:*** An employee shall not accept any item of significant monetary value (e.g., gifts, gratuity, favor, entertainment, loan, unusual discount) except usual social and business courtesies (e.g., a meal, box of candy, samples) from a person who has or is seeking to obtain a contractual or financial relationship with the employee's organizational unit or whose activities are regulated by such.

8. ***HONORARIA:*** An employee shall not accept honoraria or other compensation for activities which are, or should be, performed as part of one's official duties, except as provided by the Comprehensive Travel Regulations of the Department of Finance and Administration.

9. ***ACTION TO RESOLVE A CONFLICT OF INTEREST:*** An employee who has a conflict of interest must immediately eliminate such conflict. If an employee's activities give the appearance of a conflict of interest, such activities must be eliminated. If there is uncertainty whether a current or proposed activity is a conflict of interest, an employee should notify the Commissioner in writing of the potential conflict and receive approval for such activity.

10. ***VIOLATION OF CONFLICT OF INTEREST:*** An employee with a conflict of interest in violation of this policy is subject to disciplinary action in accordance with the Department of Personnel's rules and regulations. An employee who violates a statutory conflict of interest is also subject to sanctions provided by statute.

D HR

POLICY

Approved by: Rebecca R. Hunter, Commissioner	**Policy Number:** 12-056
Signature: Rebecca R Hunter	**Supersedes:** 11-001; 03-034
Application: Executive Branch Employees	**Effective Date:** October 3, 2012
Authority: T.C.A. § 4-3-1703, T.C.A. § 8-30-104, T.C.A. § 8-30-203, T.C.A. § 55-10-401	**Rule:** Chapter 1120-10

Subject:

Operation of Motor Vehicles By State Employees

State employees who are required to drive state-owned and/or personally-owned vehicles, or who elect to participate in the WeCar/Enterprise Program, in the course of their employment in order to perform official state functions shall do so legally, safely, and defensively. In addition, state-owned vehicles shall be operated in compliance with the policies of the Motor Vehicle Management Division in the Department of General Services and by any terms and conditions established by the WeCar/Enterprise Program. Employees are required at all times to comply with any and all laws when operating any motor vehicle on official state business.

It is of paramount importance that an employee who is in a position that requires a valid vehicle operator's license, or who operates a motor vehicle for state business, possess a valid driver's license. Regardless of whether a state, personal, or rental vehicle is being used in the course of state business, the state may be held liable for the actions of the employee. Therefore, all employees shall abide by the following:

- Any employee operating a state, personal, or rental vehicle for official state business is required to possess a valid driver's license from the employee's domicile state.
- When required, the license must have the appropriate commercial endorsement.
- Under no circumstances shall an employee whose license is revoked, suspended, expired, or otherwise invalidated operate a motor vehicle for official state business.
- For employees who are required to maintain a valid driver's license as part of their official duties, driving record convictions may be considered as grounds for disciplinary action, up to and including dismissal, whether the offenses and infractions occurred during or outside work hours. This includes driving under the influence as defined in Tenn. Code Ann. § 55-10-401.
- Any employee whose position requires a valid driver's license as a job qualification shall advise his or her supervisor within twenty-four (24) hours of the employee's next scheduled workday of any conviction, suspension, revocation, expiration, or invalidation of the employee's driver's

license. Failure to notify the supervisor of any such conviction, suspension, revocation, expiration, or invalidation may be cause for disciplinary action, up to and including dismissal.

- Any state employee who is convicted of driving under the influence in violation of Tenn. Code Ann. § 55-10-401, or of any offense for which driving under the influence is an element, while driving a state, personal, or rental vehicle on official state business, is subject to discipline, up to and including dismissal.

- An employee who is not required to possess a valid driver's license in the performance of his or her job duties may be disciplined for driving under the influence while off-duty when an agency determines that the conduct adversely impacts the employee's ability to effectively perform his or her job duties or the best interest of the state.

Appointing authorities shall be responsible for ensuring all employees receive a copy of this policy. Employees are required to sign the acknowledgement below upon receipt of this policy for inclusion in the employee's personnel file. Employees who are required to maintain a valid driver's license as part of their official duties shall provide proof of a valid driver's license at the time of acknowledgement. This policy does not restrict agencies from augmenting the provisions of this policy with additional policies and procedures.

Employees are required to complete and sign an "Operation of Motor Vehicles by State Employees" Acknowledgement form (PR-0397, attached below).

Questions regarding the portion of this policy as it pertains to employee discipline may be directed to the Employee Relations Division of the Department of Human Resources. Questions pertaining to the operation of motor vehicles should be directed to the Department of General Services.

STATE OF TENNESSEE

Acceptable Use Policy
Network Access Rights and Obligations

Purpose:
To establish guidelines for State-owned hardware and software, computer network access and usage, Internet and email usage, telephony, and security and privacy for users of the State of Tennessee Wide Area Network.

Reference:
Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994.
Tennessee Code Annotated, Section 10-7-512, effective July 1, 2000.
Tennessee Code Annotated, Section 10-7-504, effective July 1, 2001.
State of Tennessee Security Policies.

Objectives:
- Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
- Provide uninterrupted network resources to users.
- Ensure proper usage of networked information, programs and facilities offered by the State of Tennessee networks.
- Maintain security of and access to networked data and resources on an authorized basis.
- Secure email from unauthorized access.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users there is no expectation of privacy in their use of State-owned hardware, software, or computer network access and usage.
- Provide Internet and email access to the users of the State of Tennessee networks.

Scope:
This Acceptable Use Policy applies to all individuals who have been provided access rights to the State of Tennessee networks, State provided email, and/or Internet via agency issued network or system User ID's. The scope does not include State phone systems, fax machines, copiers, State issued cell phones or pagers unless those services are delivered over the State's IP network.

Use and Prohibitions:

A. Data and Information Technology Resources
State employees, vendors/business partners/subrecipients, local governments, and other governmental agencies may be authorized to access state data or Information Technology (IT) network resources to perform business functions with or on behalf of the State. Users

must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature. It is recognized that there may be incidental personal use of State IT Resources. This practice is not encouraged and employees should be aware that all usage may be monitored and that there is no right to privacy. Various transactions resulting from network usage are the property of the state and are thus subject to open records laws.

Prohibitions

- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation.
- Installing software that has not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Attaching processing devices that have not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Using data and IT resources to play or download games, music or videos that are not in support of business functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using data and IT resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing data and IT resources for activities that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.

B. Email

Email and calendar functions are provided to expedite and improve communications among network users.

Prohibitions

- Sending unsolicited junk email or chain letters (e.g. "spam") to any users of the network.
- Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
- Sending or receiving communications that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.
- Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met.

Email created, sent or received in conjunction with the transaction of official business are public records in accordance with T.C.A 10-7-301 through 10-7-308, and the rules of the Public Records Commission. A public record is defined as follows:

> *"Public record(s)" or "state record(s)" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (T.C.A. 10-7-301 (6)).*

State records are open to public inspection unless they are protected by State or Federal law, rule, or regulation. Because a court could interpret state records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail could be made available to the public.

C. Internet Access

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

- Using the Internet to access non-State provided web email services.
- Using Instant Messaging or Internet Relay Chat (IRC).
- Using the Internet for broadcast audio for non-business use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using the Internet when it violates any federal, state or local law.

Statement of Consequences

Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Statement of Enforcement

Noncompliance with this policy may result in the following immediate actions.

1. Written notification will be sent to the Agency Head and to designated points of contact in the User Agency's Human Resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance as "cause". In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
2. User access may be terminated immediately by the Systems Administrator, and the user may be subject to subsequent review and action as determined by the agency, department, board, or commission leadership, or contract administrator.